# EXHIBIT 2

**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEBRAKSA**

| | |
|---|---|
| **In re ALN Medical Management LLC Data Incident Litigation** | Case No.: 4:25-cv-3067<br><br>**CONSOLIDATED AMENDED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Inserted Cells

## CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Cameron Reed, Eugene Rosenberg, Lauren Mullis, Jeffrey Judka, Virginia Gilleland, Robert Meyers, Caroline Hurley, and Timothy Keggins bring this Class Action Complaint, against Defendants ALN Medical Management, LLC ("ALN"), Long View Systems Corporation (USA) ("LVSC"), National Spine and Pain Centers, LLC ("NSPC"), Bethany Medical Clinic of New York, PLLC ("BMC"), and Hoag Clinic ("Hoag") (collectively, Defendants"), and each of their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to their own actions, and information and belief as to all other matters, allege as follows:

### INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Defendants' current and former patients, Personally Identifying Information[1] ("PII") and

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the Data Breach.

Protected Health Information ("PHI")[2] (collectively "Private Information"), including of Plaintiffs and the Class Members, which was in Defendants' possessions in a cyberattack beginning on or around March 2024, caused by Defendants' collective failures to adequately safeguard that Private Information ("the Data Breach").

2. According to Defendants, the Private Information compromised in the Data Breach includes patients' names, dates of birth, health insurance information, demographic information, Social Security numbers, and financial information.

3. Defendant ALN is a healthcare advisory firm that provides services such as physician, facility, and non-participating provider hospital billing, professional coding, claims recovery, review of billing practices, and credentialing to clients, including to NSPC, BMC, and Hoag.[4]

4. Defendant LVSC is an IT solutions provider offering services such as workspace solutions, data modernization, cybersecurity, and cloud infrastructure to clients, including ALN.[6]

5. Defendant NSPC is a pain management practice that provides administrative services to interventional pain management clinics focused on relieving chronic back and neck

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, *inter alia*, a group health plan. *Id. Covered entity, Health plan*. A "business associate" is defined as, with respect to a covered entity, a person who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing…" *Id. Business associate*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, Dep't for Health & Hum. Servs., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 5, 2022). Bethany Medical is clearly a "covered entity," and ALN is clearly a "business associate," subject to HIPAA, and some of the PHI compromised in the Data Breach is "protected health information," subject to HIPAA.

[4] https://www.bloomberg.com/profile/company/0370828D:US?embedded-checkout=true

[6] *About Us*, Long View Systems Corporation: https://www.longviewsystems.com/about-us/journey-to-100-years/ (last visited June 19, 2025).

pain.[7]

6. Defendant BMC is a multi-specialty medical practice.[8]

7. Defendant Hoag is a regional health care delivery network offering services across primary and specialty care.[9]

8. Defendants failed to undertake adequate measures to safeguard the Private Information of Plaintiffs and the proposed Class Members.

9. Although Defendants purportedly discovered the Data Breach on March of 2024, they failed to immediately notify and warn current and former patients, with ALN waiting an entire year, until March 21, 2025, to provide written notice to Plaintiffs and the Class.

10. As a direct and proximate result of Defendants' failures to protect current and former patients' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

**PARTIES**

11. Plaintiff Cameron Reed is a natural person, resident and citizen of New York, where he intends to remain. Plaintiff Reed is a former patient of BMC, and a Data Breach victim.

12. Plaintiff Eugene Rosenberg is a natural person, resident and citizen of Florida, where he intends to remain. Plaintiff Rosenburg is a former patient of NSPC, and a Data Breach victim.

13. Plaintiff Lauren Mullis is a natural person, resident and citizen of California, where she intends to remain. Plaintiff Mullis is a former patient of Hoag, and a Data Breach victim.

[7] *About Us*, National Spine Pain Centers, LLC: https://www.treatingpain.com/about-us/ (last visited June 19, 2025).
[8] *About*, Bethany Medical Clinic: https://bmcofny.com/about/ (last visited June 19, 2025).
[9] *About Hoag*, Hoag Clinic: https://www.hoag.org/about-hoag/ (last visited June 19, 2025).

14. Plaintiff Jeffrey Judka is a natural person, resident and citizen of Pennsylvania, where he intends to remain. Plaintiff Judka is a former patient of NSPC, and a Data Breach victim.

15. Plaintiff Virginia Gilleland is a natural person, resident and citizen of Louisiana, where she intends to remain. Plaintiff Gilleland is a current patient of NSPC, and a Data Breach victim.

16. Plaintiff Robert Meyers is a natural person, resident and citizen of New Jersey, where he intends to remain. Plaintiff Meyers is a former patient of NSPC, and a Data Breach victim.

17. Plaintiff Caroline Hurley is a natural person, resident and citizen of New Jersey, where she intends to remain. Plaintiff Hurley is a former patient of NSPC, and a Data Breach victim.

18. Plaintiff Timothy Keggins is a natural person, resident and citizen of Maryland, where he intends to remain. Plaintiff Keggins is a former patient of NSPC, and a Data Breach victim.

19. Defendant ALN is a Limited Liability Company organized and existing under the laws of the State of Delaware, with its principal place of business located in Lincoln, Nebraska.

20. Defendant BMC is a professional Limited Liability Company organized and existing under the laws of the State of New York, with its principal place of business located in New York, New York.

21. Defendant NSPC is a Limited Liability Company organized and existing under the laws of the State of Delaware, with its principal place of business located in Frederick, Maryland.

22. Defendant Hoag is a nonprofit corporation organized and existing under the laws of the State of California, with its principal place of business located in Newport Beach, California.

23. Defendant LVSC is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located in Denver, Colorado.

**JURISDICTION & VENUE**

24. This Court has original jurisdiction over this action under the Class Action Fairness Act 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

25. This Court has personal jurisdiction over Defendants because Defendant ALN's principal place of business is in Nebraska, and Defendants regularly conduct business and enters into contracts within the State of Nebraska.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because ALN's principal place of business is in this District and a substantial art of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

**BACKGROUND FACTS**

**A. Defendants**

27. Defendant ALN "offers billing and claims submission, coding, compliance, month end closing, performance management, information technology, and quality management services" to physician practices across the country.[11]

28. Defendant LVSC offers services including workspace solutions, data modernization, cybersecurity, and cloud infrastructure to clients, including Defendant ALN.[13]

29. Defendants ALN and LVSC were provided with Plaintiffs' and the proposed Class

[11] https://www.bloomberg.com/profile/company/0370828D:US?embedded-checkout=true
[13] *About Us*, Long View Systems Corporation: https://www.longviewsystems.com/about-us/journey-to-100-years/ (last visited June 19, 2025).

Members' Private Information by Defendants NSPC, BMC, and Hoag.

30. Defendants NSPC, BMC, and Hoag each require that their patients provide them with their Private Information. Defendants NSPC, BMC and Hoag then provide the Private Information of patients to ALN so that ALN can render medical services.

31. Defendant ALN collects and stores Plaintiffs' and the proposed Class Members' Private Information on an IT Network managed by LSVC, including but not limited to their names, dates of birth, health insurance information, demographic information, Social Security numbers, and financial information.

32. When Defendants collect this Private Information, they promise to use reasonable care to protect and safeguard the Private Information, from unauthorized disclosure. Plaintiffs and Class Members would not have provided their Private Information to Defendants had they known that Defendants would not employ data security measures sufficient to protect the confidentiality of their Private Information.

33. Upon information and belief, Defendants maintain privacy policies in which they promise to maintain the confidentiality of individuals' Private Information.

34. Despite their alleged commitments to securing sensitive patient data, Defendants did not follow industry standard practices in securing patients' Private Information and failed to protect the Private Information of Plaintiffs and the proposed Class Members from unauthorized disclosure in the Data Breach.

**B. Defendants Fail to Safeguard Private Information—the Data Breach**

35. On information and belief, according to Defendants, beginning on or around March 2024, Defendant ALN experienced a cyberattack to its computer information technology systems managed by Defendant LSVC by an "unauthorized threat actor," which resulted in the

unauthorized disclosure and exfiltration of patients' Private Information, including of Plaintiffs and the proposed Class Members, including name, dates of birth, health insurance information, demographic information, Social Security number, and financial information—the Data Breach.[14]

36. Nevertheless, Defendants waited a ***full year*** to inform affected current and former patients of the unauthorized disclosure of their Personal Dara Breach in the Data Breach, waiting until March 2025 for ALN to provide written notice to Plaintiffs and the Class.

37. On or about March 21, 2025, Defendant ALN began sending written notice of the Data Breach to current and former patients impacted by the Data Breach, including Plaintiffs, and the proposed Class Members.[15]

2. The Data Breach Notice stated:

> In March 2024, ALN identified suspicious activity related to certain systems being hosted by a third-party service provider. Upon learning of this activity, ALN promptly took steps to ensure the security of ALN systems, isolated the impacted environment, and launched an investigation to determine the nature and scope of the activity. While the incident did not impact internal ALN systems, the investigation determined that certain files and folders within the third-party hosted environment were accessed or taken by an unauthorized actor between March 18, 2024 and March 24, 2024.[16]

38. The information involved in the Data Breach included names, dates of birth, health insurance information, demographic information, Social Security numbers, and financial information.[17]

39. In addition, in its Data Breach Notice, Defendant ALN recognized the threat of identity theft and fraud and recommended that affected persons "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports," place

[14] Exhibit A.
[15] *Id.*
[16] *Id.*
[17] *Id.*

fraud alerts and security freezes on their credits files, and contact the consumer reporting agencies.[18]

40. Defendant ALN's Data Breach Notice did not further elaborate on the nature or extent of the Data Breach, omitting its scope or size.

41. Defendants' conduct, by acts of commission or omission, caused the Data Breach, including: Defendants ALN and LVSC's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard patient Private Information, allowing Private Information to be accessed and stolen, and by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach; as well as Defendants NSPC, BMC, and Hoag's failure to ensure that their third-party vendors, Defendants ALN and LSVC, undertook these data security measures and appropriate employee training, prior to obtaining Plaintiffs and the Class Members' Private Information.

42. Had Defendants NSPC, BMC, and Hoag audited and reviewed Defendants ALN's and LSVC's data security measures they would have known that entrusting the Private Information of their patients to these third party providers created a foreseeable risk of the compromise of that Private Information. Defendants NSPC, BMC, and Hoag had a duty to ensure that any third party service provider had properly implemented and employed reasonable data security measures necessary to protect the Private Information of healthcare patients.

43. On information and belief, as more fully articulated below, Plaintiffs' and the members of the proposed Class Members' Private Information, was unauthorizedly disclosed to,

[18] *Id.*

and actually "exfiltrated by," third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and/or utilized for criminal and fraudulent purposes and misuse.

**C. Plaintiffs Experiences**

***Cameron Reed***

44. Plaintiff Cameron Reed is a former patient of Defendant BMC, who received treatment from Defendant BMC.

45. As a condition of receiving Defendant BMC's medical services, Plaintiff Reed was required to provide her Private Information to Defendant BMC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Reed's name, date of birth, health insurance information, demographic information, Social Security number, and financial information.

46. Plaintiff Reed typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Plaintiff Reed has never knowingly transmitted Private Information over the internet or other unsecured sources.

47. Plaintiff Reed stores any documents containing his Private Information in a safe and secure location, and he diligently chooses unique usernames for his passwords and online accounts.

48. In entrusting his Private Information to Defendants, Plaintiff Reed believed that, as part of the payments for medical treatment and services, Defendants BMC, ALN, and LSVC would adequately safeguard that information. Had Plaintiff Reed known that Defendants BMC, ALN, and LSVC did not utilize reasonable data security measures, and that Defendant BMC did not ensure that third-party vendors utilized reasonable data security measures, Plaintiff Reed would

not have entrusted his Private Information to said Defendants or would have paid less for those treatments and services.

49. Plaintiff Reed received Defendant ALN's Data Breach Notice dated March 21, 2025, informing him that his Private Information, including his name, date of birth, health insurance information, and demographic information was impacted and exfiltrated in the Data Breach. Private Information

50. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Reed has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff has been and will be forced to expend considerable time and effort to monitor his accounts and credit files, changing his online account passwords, verifying the legitimacy of Defendant ALN's Data Breach Notice and researching the Data Breach, to protect himself from identity theft and fraudulent misuse of her Private Information, disclosed as a result of the Data Breach.

51. In addition, because of the Data Breach, Plaintiff Reed also suffered diminution in the value of his Private Information, a form of intangible property that he entrusted to Defendants BMC, ALN and LSVC, for the sole purpose of obtaining medical services.

52. Furthermore, Plaintiff Reed has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

53. He fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized

disclosure of his Private Information. He is experiencing feelings of anxiety, embarrassment, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

54. Plaintiff Reed was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive Private Information and the harm caused by the Data Breach. He was also outraged that Defendants took a year to notify him of the Data Breach even as it was discovered in March 2024.

55. Plaintiff Reed experienced financial fraud as a result of the Data Breach, which forced him to close and obtain a new credit card due to unauthorized transactions on his account. Plaintiff Reed has also experienced a substantial uptick in spam calls, text messages, and emails because of the Data Breach.

56. As a result of the Data Breach, Plaintiff Reed faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed.

57. Furthermore, Plaintiff Reed's sensitive Private Information remains in Defendants' possession without adequate protection against known threats, exposing Plaintiff Reed to the prospect of additional harm.

***Eugene Rosenberg***

58. Plaintiff Eugene Rosenberg is a former patient of Defendant NSPC.

59. As a condition of receiving Defendant NSPC's medical services, Plaintiff Rosenberg was required to provide his Private Information to Defendant NSPC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Rosenberg's name, date of birth, health insurance information, demographic information, Social Security number, and

financial information.

60. Plaintiff Rosenberg typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Plaintiff Rosenberg has never knowingly transmitted Private Information over the internet or other unsecured sources.

61. Plaintiff Rosenberg stores any documents containing his Private Information in a safe and secure location, and he diligently chooses unique usernames for his passwords and online accounts.

62. In entrusting his Private Information to Defendants, Plaintiff Rosenberg believed that, as part of the payments for medical treatment and services, Defendants NSPC, ALN and LSVC, would adequately safeguard that information. Had Plaintiff Rosenberg known that said Defendants did not utilize reasonable data security measures, and that Defendant NSPC did not ensure that third-party vendors utilized reasonable data security measures, Plaintiff Rosenberg would not have entrusted his Private Information to said Defendants or would have paid less for those treatments and services.

63. Plaintiff Rosenberg received Defendant ALN's Data Breach Notice on or around March 2025, informing him that his Private Information was impacted and exfiltrated in the Data Breach.

64. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Rosenberg has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff Rosenberg has been and will be forced to expend considerable time and

effort to monitor his accounts and credit files, changing his online account passwords, verifying the legitimacy of Defendant ALN's Data Breach Notice and researching the Data Breach, to protect himself from identity theft and fraudulent misuse of her Private Information, disclosed as a result of the Data Breach.

65. In addition, because of the Data Breach, Plaintiff Rosenberg also suffered diminution in the value of his Private Information, a form of intangible property that he entrusted to Defendants NPSC, ALN and LSVC, for the sole purpose of obtaining medical services.

66. Furthermore, the Data Breach has caused Plaintiff Rosenberg significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information.

67. He fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. He is experiencing feelings of anxiety and stress because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

68. Plaintiff Rosenberg was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive Private Information and the harm caused by the Data Breach. He was also outraged that Defendants took a year to notify him of the Data Breach even as it was discovered in March 2024.

69. Since the Data Breach occurred, Plaintiff Rosenberg has experienced a significant uptick in spam calls. Furthermore, Plaintiff Rosenberg experienced a fraudulent charge on his bank card, that resulted in the charge being disputed and his card replaced, which Plaintiff Rosenberg reasonably believes is attributable to the Data Breach.

70. As a result of the Data Breach, Plaintiff Rosenberg faces a lifetime risk of identity

theft, as it includes sensitive information that cannot be changed.

71. Furthermore, Plaintiff Rosenberg's sensitive Private Information remains in Defendants' possession without adequate protection against known threats, exposing Plaintiff Rosenberg to the prospect of additional harm.

***Lauren Mullis***

72. Plaintiff Lauren Mullis is a former patient of Hoag, who received treatment from Defendant Hoag.

73. As a condition of receiving Defendant Hoag's medical services, Plaintiff Mullis was required to provide her Private Information to Defendant Hoag, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Mullis' name, dates of birth, health insurance information, demographic information, Social Security number, and financial information.

74. Plaintiff Mullis typically takes measures to protect her Private Information and is very careful about sharing his Private Information. Plaintiff Mullis has never knowingly transmitted Private Information over the internet or other unsecured source.

75. Plaintiff Mullis stores any documents containing her Private Information in a safe and secure location, and she diligently chooses unique usernames for her passwords and online accounts.

76. In entrusting her Private Information to Defendants Hoag, ALN and LSVC, Plaintiff Mullis believed that, as part of the payments for medical treatment and services, said Defendants would adequately safeguard that information. Had Plaintiff Mullis known that Defendants Hoag, ALN and LSVC did not utilize reasonable data security measures, she would not have entrusted her Private Information to said Defendants or would have paid less for those

treatments and services.

77. Plaintiff Mullis received Defendant ALN's Data Breach Notice dated March 21, 2025, informing her that her Private Information, including her name, date of birth, health insurance information, and demographic information was impacted and exfiltrated in the Data Breach.

78. As a direct and proximate result of the Data Breach permitted to occur by Defendants Hoag, ALN and LSVC, Plaintiff Mullis has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff Mullis has been and will be forced to expend considerable time and effort to monitor her accounts and credit files, changing her online account passwords, verifying the legitimacy of Defendant ALN's Data Breach Notice and researching the Data Breach, to protect herself from identity theft and fraudulent misuse of her Private Information, disclosed as a result of the Data Breach.

79. In addition, as a result of the Data Breach, Plaintiff Mullis also suffered diminution in the value of her Private Information, a form of intangible property that she entrusted to Defendants Hoag, ALN, and LSVC for the sole purpose of obtaining medical services.

80. Furthermore, Plaintiff Mullis has experienced significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data Breach.

81. She fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized

disclosure of her Private Information. She is experiencing feelings of anxiety, embarrassment, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

82. Plaintiff Mullis was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and the harm caused by the Data Breach. She was also outraged that Defendants took a year to notify her of the Data Breach even as it was discovered in March 2024. 45. As a result of the Data Breach, Plaintiff Mullis faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed.

83. Furthermore, Plaintiff Mullis sensitive Private Information remains in Defendants Hoag, ALN and LSVC's possession without adequate protection against known threats, exposing Plaintiff Mullis to the prospect of additional harm.

***Jeffrey Judka***

84. Plaintiff Jeffrey Judka is a former patient of NSPC.

85. As a condition of receiving Defendant NSPC's medical services, Plaintiff Judka was required to provide his Private Information to Defendant NSPC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Judka's name, dates of birth, health insurance information, demographic information, Social Security number, and financial information.

86. Plaintiff Judka had the reasonable expectation and mutual understanding that said Defendants would keep his Private Information secure from unauthorized access.

87. By soliciting and accepting Plaintiff Judka's Private Information, Defendants NSPC, ALN and LSVC agreed to safeguard and protect it from unauthorized access and delete it

after a reasonable time.

88. Defendants NSPC, ALN and LSVC were in possession of Plaintiff Judka's Private Information before, during, and after the Data Breach.

89. Plaintiff Judka is a victim of the Data Breach whose Private Information was stolen therein.

90. Following the Data Breach, Plaintiff Judka made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. In total, Plaintiff Judka estimates he has already spent 100 hours responding to the Data Breach.

91. Plaintiff Judka will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent, which has been lost forever and cannot be recaptured.

92. Plaintiff Judka places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Judka has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

93. As a result of the Data Breach, Plaintiff Judka has experienced an uptick in spam calls, texts messages, and email.

94. As a direct and traceable result of the Data Breach, Plaintiff Judka suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because Defendants did not adequately protect his Private Information; (d) emotional distress because identity thieves now

possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendants obtained from Plaintiff Judka and/or his medical providers; and (g) other economic and non-economic harm.

95. Plaintiff Judka has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

96. Plaintiff Judka has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Judka's Private Information will be wholly unprotected and at-risk of future data breaches.

***Virginia Gilleland***

97. Plaintiff Virginia Gilleland is a current patient of Defendant NSPC.

98. As a condition of receiving Defendant NSPC's medical services, Plaintiff Gilleland was required to provide her Private Information to Defendant NSPC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Gilleland's name, dates of birth, health insurance information, demographic information, Social Security number, and financial information.

99. Plaintiff Gilleland is a victim of the Data Breach whose Private Information was stolen therein.

100. By soliciting and accepting Plaintiff Gilleland's Private Information, Defendants NSPC, ALN and LSVC agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

101. Defendants NSPC, ALN and LSVC were in possession of Plaintiff Gilleland's Private Information before, during, and after the Data Breach.

102. The Data Breach caused Plaintiff Gilleland's Private Information to be compromised by unauthorized third parties.

103. Plaintiff Gilleland is very careful about sharing her sensitive Private Information and diligently maintains her Private Information in a safe and secure manner. Plaintiff Gilleland has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

104. As a result of the Data Breach, Plaintiff Gilleland has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

105. Plaintiff Gilleland has suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff Gilleland cannot be undone.

106. As a result of the Data Breach, Plaintiff Gilleland has experienced an uptick in spam calls, text messages, and emails.

107. Plaintiff Gilleland further suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff

Gilleland entrusted to Defendants, which was compromised in and as a result of the Data Breach.

108. Plaintiff Gillleland has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of cybercriminals.

109. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

110. Plaintiff Gilleland has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants control, is protected, and safeguarded from future breaches.

***Robert Meyers***

111. Plaintiff Robert Meyers is a former patient of Defendant NSPC.

112. As a condition of receiving Defendant NSPC's medical services, Plaintiff Meyers was required to provide his Private Information to Defendant NSPC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Meyers' name, date of birth, health insurance information, demographic information, Social Security number, and financial information.

113. Plaintiff Meyers typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Plaintiff Meyers has never knowingly transmitted Private Information over the internet or other unsecured sources.

114. Plaintiff Meyers stores any documents containing his Private Information in a safe and secure location, and he diligently chooses unique usernames for his passwords and online accounts.

115. In entrusting his Private Information to Defendants, Plaintiff Meyers believed that,

as part of the payments for medical treatment and services, Defendants NSPC, ALN and LSVC, would adequately safeguard that information. Had Plaintiff Meyers known that said Defendants did not utilize reasonable data security measures, and that Defendant NSPC did not ensure that third-party vendors utilized reasonable data security measures, Plaintiff Meyers would not have entrusted his Private Information to said Defendants or would have paid less for those treatments and services.

116. Plaintiff Meyers received Defendant ALN's Data Breach Notice on or around March 2025, informing him that his Private Information was impacted and exfiltrated in the Data Breach.

117. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Meyers has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff Rosenberg has been and will be forced to expend considerable time and effort to monitor his accounts and credit files, changing his online account passwords, verifying the legitimacy of Defendant ALN's Data Breach Notice and researching the Data Breach, to protect himself from identity theft and fraudulent misuse of her Private Information, disclosed as a result of the Data Breach.

118. In addition, because of the Data Breach, Plaintiff Meyers also suffered diminution in the value of his Private Information, a form of intangible property that he entrusted to Defendants NPSC, ALN and LSVC, for the sole purpose of obtaining medical services.

119. Furthermore, the Data Breach has caused Plaintiff Meyers significant worry and

feelings of anxiety and emotional distress regarding the disclosure of his Private Information.

120. He fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. He is experiencing feelings of anxiety and stress because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

121. Plaintiff Meyers was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive Private Information and the harm caused by the Data Breach. He was also outraged that Defendants took a year to notify him of the Data Breach even as it was discovered in March 2024.

122. Since the Data Breach occurred, Plaintiff Meyers has experienced a significant uptick in spam calls. The spam messages impersonate legitimate business entities and request his personal information.

123. As a result of the Data Breach, Plaintiff Meyers faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed.

124. Furthermore, Plaintiff Meyers' sensitive Private Information remains in Defendants' possession without adequate protection against known threats, exposing Plaintiff Meyers to the prospect of additional harm.

***Caroline Hurley***

125. Plaintiff Carolien Hurley is a former patient of Defendant NSPC.

126. As a condition of receiving Defendant NSPC's medical services, Plaintiff Hurley was required to provide her Private Information to Defendant NSPC, which it then provided to Defendants ALN and LSVC, including but not limited to Plaintiff Hurley's name, dates of birth,

health insurance information, demographic information, Social Security number, and financial information.

127. Plaintiff Hurley is a victim of the Data Breach whose Private Information was stolen therein.

128. By collecting and maintaining Plaintiff Hurley's Private Information, Defendants NSPC, ALN and LSVC agreed to safeguard her data using reasonable means according to their internal policies, as well as state and federal law.

129. Plaintiff Hurley was deprived of the earliest opportunity to guard herself against the Data Breach's effects due to Defendants' failure to notify her about the breach for about a year.

130. As a result of their inadequate cybersecurity, Defendants NSPC, ALN and LSVC exposed Plaintiff Hurley's Private Information for theft by cybercriminals and sale on the dark web.

131. As a result of the Data Breach notice, Plaintiff Hurley has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

132. Plaintiff Hurley has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Hurley fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

133. Plaintiff Hurley has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry

or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

134. Plaintiff Hurley has suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Hurley entrusted to Defendants NSPC, ALN and LSVC, which was compromised in and as a result of the Data Breach.

135. Plaintiff Hurley has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

136. Indeed, following the Data Breach, Plaintiff Hurley has experienced a large increase in phishing calls, experiencing over 10 calls a day suggesting that her Private Information is now in the hands of cybercriminals. As a result of this enormous increase, Plaintiff Hurley was forced to purchase an internet protection program through Netgear, with the hopes to either stop the spam calls entirely or at least have these calls identified as spam on her cellphone.

137. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Hurley's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

138. On information and belief, the phishing calls Plaintiff Hurley is experiencing were made possible as a result of the Data Breach and the subsequent exposure of Plaintiff Hurley's Personal information to cybercriminals.

139. Plaintiff Hurley has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants possession, is protected, and safeguarded from future breaches.

***Timothy Keggins***

140. Plaintiff Timothy Keggins is a former patient of Defendant NSPC.

141. As a condition of receiving Defendant NSPC's medical services, Plaintiff Keggins was required to provide her Private Information to Defendant NSPC, which it then provided to Defendants ALN, LSVC, and NSPC, including but not limited to Plaintiff Keggins' name, dates of birth, health insurance information, and demographic information.

142. Plaintiff Keggins is a victim of the Data Breach whose Private Information was stolen therein.

143. By collecting and maintaining Plaintiff Keggins' Private Information, Defendants NSPC, LSVC, and ALN agreed to safeguard his data using reasonable means according to their internal policies, as well as state and federal law.

144. Plaintiff Keggins was deprived of the earliest opportunity to guard himself against the Data Breach's effects due to Defendants' failure to notify her about the breach for about a year.

145. As a result of their inadequate cybersecurity, Defendants NSPC, LSVC, and ALN exposed Plaintiff Keggins' Private Information for theft by cybercriminals and sale on the dark web.

146. As a result of the Data Breach notice, Plaintiff Keggins has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

147. Plaintiff Keggins has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Keggins fears for his personal

financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

148. Plaintiff Keggins has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

149. Plaintiff Keggins has suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Keggins entrusted to Defendants NSPC, LSVC, and ALN which was compromised in and as a result of the Data Breach.

150. Plaintiff Keggins has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

151. Indeed, following the Data Breach, Plaintiff Keggins had multiple debit and credit cards opened in his name. Plaintiff Keggins has spent hours addressing this fraudulent activity.

152. To make matters worse, on May 21, 2025, Plaintiff Keggins was notified that an unauthorized individual was attempting to tender payment for multiple medical procedures using his name and financial account information.

153. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Keggins' Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

154. Plaintiff Keggins has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants possession, is protected, and

safeguarded from future breaches.

**C. This Data Breach was Foreseeable by Defendants.**

155. Plaintiffs and the proposed Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

156. By failing to do so, Defendants put Plaintiffs and Class Members at risk of identity theft, financial fraud, and other harms.

157. Defendants tortiously, or in breach of their implied contracts, failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiffs and the Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiffs and the other Class Members' rights.

158. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

159. According to a Chief Strategy Officer at ClearDATA, "[i]t's no secret that healthcare is the industry most plagued by data breaches. Patient data is the most valuable, making it targeted by bad actors."[20]

160. Moreover, healthcare companies are targeted because of their cybersecurity vulnerabilities: "…healthcare is also targeted because it is very vulnerable. Many healthcare

[20] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last visited. June 19, 2025).

providers use outdated IT infrastructure and operating systems that can no longer be patched or supported, such as Windows 7 and Windows Server 2008, even after Microsoft retired them. Further, more than half of medical devices operate on legacy systems, and 83% of medical imaging devices are on outdated operating systems that no longer receive patches/updates. This creates significant cybersecurity vulnerabilities and makes it much easier for bad actors to find an entry point into the network." [21]

161. Cyber-attacks against healthcare organizations such as Defendants are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors…"[22]

162. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[23]

163. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[24]

164. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security

[21] *Id.*
[22] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited June 19, 2025)
[23] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited June 19, 2025)
[24] *Ibid.*

numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[25]

165. According to the ITRC's January 2023 report for 2022, "[t]he number of publicly reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises."[26] In 2022, there were approximately 422 million individuals affected by cyberattacks.[27]

166. Moreover, of the 1,802 data breaches in 2022, ITRC reported that 1,560 involved compromised names, 1,143 involved compromised of Social Security Numbers, and 633 involved compromised dates of birth—types of PHI included in the unauthorized disclosure in this Data Breach.[28]

167. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[29]

168. Furthermore, Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported medical or healthcare data breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[30]

---

[25] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited June 19, 2025).
[26] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 7 (last visited June 19, 2025).
[27] *See Id*., pg. 2.
[28] *Id*., pg. 6.
[29] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last visited June 19, 2025).
[30] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022), at pg. 15.

169. According to the U.S. Department for Health and Human Services' "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," "[h]ealthcare data breaches have doubled in 3 years."[31]

170. PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

171. PHI can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

172. Given the nature of the Data Breach, it was foreseeable that the compromised Private Information could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Class Members' PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

**D. Defendants Failed to Comply with FTC Guidelines**

173. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

174. In 2016, the FTC updated its publication, *Protecting PHI: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses

[31] U.S. Department for Health and Human Services, The Health Sector Cybersecurity Coordination Center (HC3), "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," February 9, 2023, avail. at https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

should protect the personal customer information that they keep; properly dispose of PHI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[32]

175. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

176. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

177. These FTC enforcement actions include actions against entities failing to safeguard PHI such as Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that

[32] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last visited June 19, 2025).
[33] *See id*.

LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

178. Defendants failed to implement basic data security practices that are widely employed throughout the healthcare industry. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

179. Defendants were at all times fully aware of their obligations to protect the Private Information of its current and former patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

**E. Defendants Fail to Comply with Industry Standards**

180. As shown above, experts studying cyber security routinely identify organizations holding PHI as being particularly vulnerable to cyber-attacks because of the value of the information they collect and maintain. As of 2024, the global average cost of a data breach rose by 10% over the prior year to $4.9 million.[34]

181. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery,

[34] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last visited June 19, 2025)/

Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[35]

182. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[36]

183. Upon information and belief, Defendants failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with

[35] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last visited June 19, 2025).
[36] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last visited June 19, 2025).

other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

**F. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages**

184. Plaintiffs and members of the proposed Class have suffered injury and damages from the unauthorized disclosure of their Private Information in the Data Breach that can be directly traced to Defendants ALN and LSVC's failure to adequately protect that Private Information, and Defendants NSPC, BMC, and Hoag's failures to ensure Defendants ALN and LSVC adequately protected that Private Information, that has occurred, is ongoing, and/or imminently will occur.

185. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access Plaintiffs' and the proposed Class Members' Private Information, which on information and belief is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale, causing widespread injury and damages.

186. The ramifications of Defendants' failure to keep Plaintiffs' and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

187. Because Defendants collectively failed to prevent the Data Breach, Plaintiffs and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class Members have suffered, are at an increased risk of suffering, or will imminently suffer:

a. dissemination of that Private Information, including said information being

posted on the Dark Web for fraudulent, criminal activity or sale;

b. fraudulent misuse of Private Information, including fraudulent loans taken out using Private Information acquired in the Data Breach, fraudulent cellular telephone accounts taken out using Private Information acquired in the Data Breach; and, identity theft and impersonation using Private Information acquired in the Data Breach;

c. Targeted phishing, malware, and increase in spam emails, texts, and calls which are attempts to acquire further information to be used for fraud and identity theft;

d. The loss of the opportunity to control how their Private Information is used;

e. The diminution in value of their Private Information;

f. The compromise and continuing publication of their Private Information;

g. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

h. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

i. Emotional Distress;

j. Delay in receipt of tax refund monies;

k. Unauthorized use of stolen Private Information; and

l. The continued risk to their Private Information, which remains in the

possession of Defendants and is subject to further breaches so long as ALN fails to undertake the appropriate measures to protect the Private Information in its possession, and Bethany Medical to ensure ALN undertakes these measures.

188. Furthermore, the Data Breach has placed Plaintiffs and the proposed Class Members at an increased risk of fraud and identity theft.

189. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[37]

190. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[37] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last visited June 19, 2025).

charges from their accounts, seeking a credit freeze, and correcting their credit reports.[38]

191. The time-consuming process recommended by the FTC and other experts is complicated by the vulnerable situations of Defendants' patients.

192. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

193. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

194. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

195. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated. [39]

[38] *See* https://www.identitytheft.gov/Steps (last accessed September 1, 2021).
[39] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last visited June 19, 2025).

196. What's more, theft of Private Information is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Private Information is a valuable property right.[40]

197. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PHI has considerable market value.

198. Theft of Private Information, in particular, is problematic because: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[41]

199. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Private Information to adjust their insureds' medical insurance premiums.

200. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

---

[40] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[41] *See Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

201. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

202. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

203. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial and medical accounts for many years to come.

204. According to cybersecurity experts, "[r]eports show the value of a health record can be worth as much as $1,000, whereas on the dark web, a credit card number is worth $5 and Social Security numbers are worth $1."[42]

205. Social Security numbers are among the worst kind of PHI to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[43]

206. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for

[42] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last visited June 19, 2025).

[43] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 19, 2025)

unemployment benefits, or apply for a job using a false identity.[44] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

207. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

208. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[46] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[47]

209. Accordingly, the Data Breach has caused Plaintiffs and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages

[44] *See id.*
[45] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 19, 2025).
[46] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 19, 2025).
[47] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited June 19, 2025).

as set forth in the preceding paragraphs.

210. Defendants knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and Defendants ALN and LSVC should have strengthened their data systems accordingly, and Defendants NSPC, BMC, and Hoag should have ensured that Defendants ALN and LSVC did so before Plaintiffs and the Class Members entrusted them with their Private Information.

**CLASS ACTION ALLEGATIONS**

211. Plaintiffs bring this action on behalf of themselves, and on behalf of all other persons similarly situated on (the "Class"):

> **Nationwide:** All persons identified by Defendants (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class")
>
> **California Subclass:** All residents of California, Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "California Subclass")

212. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

213. Plaintiffs reserve the right to amend or modify the Class definitions as this case progresses.

214. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

215. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law

and fact include, without limitation:

a. if Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members' Private Information;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendants owed a duty to Class Members to safeguard their Private Information;

f. if Defendants breached their duty to Class Members to safeguard their Private Information;

g. if Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendants should have discovered the Data Breach sooner;

i. if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. if Defendants' conduct were negligent;

k. if Defendants' breach implied contracts with Plaintiffs and Class Members;

l. if Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. if Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive

damages, treble damages, and/or injunctive relief.

216. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs information, like that of every other Class Member, were compromised in the Data Breach.

217. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

218. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

219. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

220. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

221. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition

of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. if Defendants failed to timely notify the public of the Data Breach;

b. if Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. if Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendants' failure to institute adequate protective security measures amounted to negligence;

e. if Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

222. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

**COUNT I**
**NEGLIGENCE**
**(On Behalf of Plaintiffs and the Nationwide Class)**

223. Plaintiffs repeat and re-allege paragraphs 1 through 222 of this Complaint and incorporate them by reference herein.

224. Plaintiffs and the Class Members entrusted their Private Information to Defendants.

225. Defendants owed Plaintiffs and Class Members a duty to exercise reasonable care in handling and using the Private Information in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the

Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

226. Further, Defendants owed Plaintiffs and Class Members a duty to exercise reasonable care in supervising third-party vendors to ensure that their Private Information was adequately protected.

227. Defendants owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failure to collectively adequately safeguard the Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs and members of the Class's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

228. Defendants owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

229. Defendants owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew

or should have known would suffer injury-in-fact due to Defendants inadequate security protocols. Defendants sought and obtained Plaintiffs and members of the Class's Private Information.

230. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access their databases containing the Private Information—whether by a sophisticated cyberattack or otherwise.

231. Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it, and of Defendants NSPC, BMC and Hoag's supervision of third-party vendors handling of that information.

232. Defendants breached their duties by failing to exercise reasonable care in supervising its agents, employees, contractors, vendors, and suppliers, and in handling and securing the Personally Information of Plaintiffs and Class Members, which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury-in-fact and damages.

233. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-fact.

234. As a direct, proximate, and traceable result of Defendants' negligence, Plaintiffs have suffered or will imminently suffer injury-in-fact and damages, as set forth in the preceding paragraphs.

235. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including: exposure of that Private Information, including being posted on the Dark Web for fraudulent, criminal activity or sale; fraudulent misuse of Private Information including fraudulent loans, fraudulent cellular telephone accounts, and identity theft and impersonation using Private Information acquired in the Data Breach; malware, and increase in spam emails; loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; emotional Distress; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants' fail to undertake the appropriate measures to protect the Private Information in their possession; and, an increased risk of fraud and identity theft.

**~~COUNT II~~**

236. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's Private Information.

237. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients'

PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs and the members of the Class's sensitive Private Information.

238. Defendants violated their respective duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Plaintiffs and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to patients in the event of a breach, which ultimately came to pass.

239. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

240. Defendants had a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's Private Information, and to supervise third-party vendors, to ensure they did the same.

241. Defendants breached their respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's Private Information.

242. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations including HIPAA constitutes negligence *per se*.

243. As a result of the negligence of Defendants, Plaintiffs and the Class Members are

entitled to recover actual, compensatory, and punitive damages.

244. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) properly notify affected victims of the Data Breach (ii) strengthen their data security systems and monitoring procedures; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) provide adequate credit monitoring to all Class Members.

245. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the Private Information maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the exposure of the Private Information of Plaintiffs and the Class Members.

**COUNT II**
~~**COUNT III**~~
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiffs and the Nationwide Class)**

246. Plaintiffs repeat and re-allege paragraphs 1 through 222 of this Complaint and incorporate them by reference herein.

247. Plaintiffs bring this count individually and on behalf of the Class against Defendants NSPC, BMC, and Hoag ("Defendants" for the purposes of this Count).

248. Defendants offered to provide services to Plaintiffs and the Class Members in exchange for their Private Information and in exchange for amounts paid for medical treatment and services that included payment for data security.

249. Defendants entrusted the Private Information of Plaintiff and the proposed Class Members to third-party vendors.

250. Plaintiffs and the Class Members accepted Defendants offer by providing Private

Information to Defendants, and in turn to third-party vendors, in exchange for medical services.

251. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Defendants agreed they would not disclose the Private Information they collect to unauthorized persons and that they would safeguard patient Private Information.

252. Implicit in the parties' agreement was that Defendants would provide Plaintiffs and the Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

253. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an agreement.

254. Defendants materially breached the contract(s) each had entered into with Plaintiffs and the Class Members by failing to safeguard their Private Information, including the failure to supervise third-party vendors to ensure Private Information was properly safeguarded, and by failing to notify Plaintiff and Class Members promptly of the Data Breach. Defendants further breached the implied contracts with Plaintiffs fand the Class Members by:

o. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

p. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendants created, received, maintained, and transmitted.

255. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendants' material breaches of its agreement(s).

256. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

257. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

258. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

259. Defendants failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

260. In these and other ways, Defendants violated their duties of good faith and fair dealing.

261. Plaintiffs and the Class Members have sustained injury-in-fact and damages because of Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing.

262. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and the proposed Class Members and are entitled to actual, compensatory, and consequential damages.

**COUNT III**
~~**COUNT IV**~~
**THIRD-PARTY BENEFICIARY**
**(On Behalf of Plaintiffs and the Nationwide Class)**

263. Plaintiffs repeat and re-allege paragraphs 1 through 222 of this Complaint and

incorporate them by reference herein.

264. Plaintiffs and the proposed Class Members are third-party beneficiaries of contracts between NSPC, BMC, Hoag and ALN and LSVC, and likely between ALN, LSVC and other medical providers, under which ALN and LSVC: received Plaintiffs' and the Class's Private Information; stored that information in its computer network systems; and provided medical billing and revenue cycle management services to their medical service providers.

265. Plaintiffs and the proposed Class Members, as patients of NSPC, BMC, and Hoag or other parties in contract with ALN and LSVC, were the intended beneficiaries of these contracts, in that the contracts all related to the provision of medical services to Plaintiffs and the Class.

266. Defendants breached the foregoing contracts by failing to adequately protect Plaintiffs and the Class Members' Private Information, resulting in the Data Breach, and injury-in-fact and damages.

267. Defendants each materially breached the contract(s) each had entered into by failing to safeguard the Private Information entrusted to it, including by Defendants NSPC, BMC, and Hoag to properly supervise third-party vendors to ensure they safeguarded Plaintiffs and Class Members Private Information, and including breaches of the covenant of good faith and fair dealing.

268. As a direct and proximate result, Plaintiffs and Class Members are entitled to actual, compensatory, and consequential damages.

**COUNT IV**
**UNJUST ENRICHMENT**
**(On Behalf of Plaintiffs and the Nationwide Class)**

269. Plaintiffs repeat and re-allege paragraphs 1 through 222 of this Complaint and incorporate them by reference herein.

270. This claim is pleaded as the alternative to the breach of implied contractual duty claim.

271. Plaintiffs and the Class Members conferred a benefit upon Defendants in the form of monies paid for medical treatment services and by providing their Private Information to Defendants in order to receive such services.

272. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiffs and the Class Members.

273. As a result of Defendants' conduct, Plaintiffs and members of the Class suffered actual damages in an amount equal to the difference in value between the purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and the Class Members paid for, and the purchases without unreasonable data privacy and security practices and procedures that they received.

274. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs and the proposed Class Members' payments and their Private Information because Defendants failed to adequately protect their Private Information, and because Defendants NSPC, BMC, and Hoag failed to properly supervise ALN, who in turn, failed to properly supervise LSVC, to ensure Plaintiffs and the Class Members' Private Information was protected. Plaintiffs and the Class Members would not have provided their Private Information, nor used and paid for Defendants' services, had they known Defendants would not adequately protect their Private Information.

275. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

**COUNT VIII**
**Violations of the California Consumer Privacy Act ("CCPA")**
**Cal. Civ. Code § 1798.150**
**(On Behalf of Plaintiffs and the California Subclass)**

276. Plaintiff Mullis hereby repeats and realleges paragraphs 1 through 222 of this Complaint and incorporate them by reference herein.

277. Plaintiff Mullis brings this Count on her own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count) against Defendants ALN and Hoag ("Defendants" for the purposes of this Count).

278. Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs and the California Subclass's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

279. Defendants are each a "business" under the meaning of Civil Code § 1798.140 because Defendants are a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d). 219. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold Private Information, including Plaintiffs and California Subclass members' PII. Plaintiffs and California Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendants have demonstrated a pattern of failing to

adequately safeguard this information.

280. Pursuant to California Civil Code § 1798.150(b), Plaintiff Mullis mailed a CCPA notice letter to Defendants registered service agents, detailing the specific provisions of the CCPA that Defendants have violated and continue to violate. As Defendants have not cured within 30 days—and Plaintiffs believe such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

281. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

282. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually, and on behalf of all others similarly situated individually, request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing Plaintiffs' counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the

interests of Plaintiffs and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

**JURY DEMAND**

Plaintiffs demand a trial by jury on all issues so triable.

Dated: June 24, 2025 Respectfully submitted,

*/s/ Andrew J. Shamis*
Andrew J. Shamis
**SHAMIS & GENTILE, P.A.**
14 NE 1st Avenue, Suite 705
Miami, Florida 33132
ashamis@shamisgentile.com

Jeff Ostrow
**KOPELOWITZ OSTROW, P.A.**
One W Las Olas Blvd., Suite 500
Ft. Lauderdale, FL 33301
Tel: 954-332-4200
ostrow@kolawyers.com

John J. Nelson
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC**
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Interim Co-Lead Class Counsel

*pro hac vice* forthcoming